IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

1. ROBERT LEGG, individually and on behalf of all similarly situated persons, Plaintiff, v. 1. LEADERS LIFE INSURANCE COMPANY, Defendant.	Case No. CIV-21-655-D **PLAINTIFF'S FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Robert Legg ("Mr. Legg" or "Plaintiff Legg"), individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this First Amended Class Action Complaint against Defendant Leaders Life Insurance Company ("Leaders Life") and alleges as follows:

INTRODUCTION

1. Part of the bargain of obtaining Leaders Life products is turning over valuable personal identifying information ("PII"),[1] including names, Social Security

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

numbers, Tax ID numbers, birthdates and addresses, to Leaders Life, in exchange for an assurance that such highly sensitive information would be kept protected from unauthorized disclosure.

2. Identity thieves can use this information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in myriad schemes, all of which can cause grievous financial harm, negatively impact the victim's credit scores for years, and cause victims to spend countless hours mitigating the impact.

3. Every year millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers' data.

4. Leaders Life, which services over 700 agents and brokers, and 1,400 employer groups, is now among those companies which have failed to meet their obligation to protect the sensitive PII entrusted to them by their current and former customers.

5. As reported by Leaders Life, between November 25 and November 27, 2020, an unknown third party gained unauthorized access and exfiltrated certain folders on Leaders Life's systems containing customers' highly sensitive and unencrypted PII, including customer names, Social Security numbers, and Tax ID numbers.

6. Defendant Leaders Life required its customers to provide it with their sensitive PII. Defendant had an obligation to secure that PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiff

and Class Members[2] and Leaders Life.

7. As a result of Leaders Life's failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized cybercriminals who will use their PII to commit fraud and identity theft in order to profit off of the Data Breach. Plaintiff and the Class are now at much higher risk of identity theft and of cybercrimes of all kinds, especially considering the highly sensitive PII stolen here.

8. This risk constitutes a concrete injury suffered by Plaintiff and the Class, as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft continues to be recognized by numerous circuit courts across the country as a concrete injury sufficient to establish Article III standing.[3]

---

[2] As used herein, the terms "Class" or "Class Members" means the putative Nationwide Class and Maryland Subclass defined below.

[3] *See, e.g., Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact for data breach case and defining "actual misuse" as a "fraudulent charge"); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (finding plaintiffs established Article III standing by alleging imminent injuries, reasoning "it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the [] data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (standing conferred based on alleged fraudulent use of identifying information, without alleged unreimbursed expenses, because "the Supreme Court long ago made clear that 'in interpreting injury in fact ... standing [is] not confined to those who [can] show economic harm.'"); *In re Equifax, Inc. Customer Data Security Breach Litigation*, No. 20-10249, 2021 WL 2250845, at *6 (11th Cir. June 3, 2021) (holding that the plaintiffs plausibly alleged injury in fact and established standing "given the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of

9. Furthermore, Plaintiff and the Class, as also set forth below, will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

THE PARTIES

10. Defendant Leaders Life is an Oklahoma corporation that operates in 11 states across the country and is currently seeking licensure in Georgia and North Carolina.[4] Although its corporate headquarters is in Tulsa, Oklahoma, Leaders Life has a substantial presence in Oklahoma City doing business at 8510 S. Pennsylvania Avenue, Suite B, in Oklahoma City, Oklahoma.

11. Leaders Life has evolved over the years into a well-respected national life insurance company, touting on its website its primary core value, "Take Care of the Customer and the Customer Will Take Care of You."[5] Unfortunately for Plaintiff and the Class, Leaders Life failed to live up to this core value as it relates to customer data security and privacy. Leaders Life, simply stated, failed to adequately secure Plaintiff's and the Class Members' PII.

---

data…"); *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021) (recognizing that plaintiffs may establish Article III standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017) ("The principal question, then, is whether the plaintiffs have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have."); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (standing conferred based on plaintiffs' allegation of increased risk of future identity theft, holding that such allegations constituted sufficient injury-in-fact for purposes of Article III standing).

[4] *See* https://www.leaderslife.com/About_Leaders_Life.aspx (last accessed June 24, 2021).

[5] *Id.*

12. Plaintiff Legg is a resident of Fallston, Maryland and has been a customer of Leaders Life for approximately twenty (20) years.

13. Mr. Legg reasonably believed Leaders Life would keep his PII secure. Had Leaders Life disclosed to him that his PII would not be kept secure and would be easily accessible to hackers and third parties, he would not have done business with Leaders Life and would have taken additional precautions relating to his PII.

JURISDICTION AND VENUE

14. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendant because it is headquartered in Oklahoma and has sufficient minimum contacts with Oklahoma.

16. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of its business in this District and Defendant has caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

A. Leaders Life collects and stores thousands of current and former customers' PII and failed to provide adequate data security to protect it.

17. Leaders Life is a well-respected national insurance company, currently operating in eleven (11) states and seeking licensure in Georgia and North Carolina.

18. Leaders Life claims it "believe[s] in … taking care of the customer and their

needs with integrity, care, and hard work."[6]

19. Between November 25 and November 27, 2020, Leaders Life was the target of an attack by a third-party who accessed and removed from Leaders Life computer systems certain folders containing Plaintiff's and Class Members' highly sensitive PII.

20. This incident is referred to herein as the "Data Breach."

21. Leaders Life, for some yet unexplained reason, waited nearly seven (7) months from knowing of the Data Breach to send a letter to Plaintiff informing him of the data breach (the "Notice Letter" dated June 16, 2021 is attached hereto as **Exhibit 1**). The Notice Letter stated, in part, the following:

> **What Happened?**
>
> On November 27, 2020, Leaders Life learned that it was the target of a cybercriminal attack and that portions of our computer network were infected with malware. We immediately took systems offline and, with the assistance of third-party forensic specialists, launched an investigation to determine the nature and scope of the incident. The investigation confirmed that certain folders on our systems may have been accessed or removed from our systems without authorization between November 25 and November 27, 2020. We therefore undertook a lengthy and time-intensive, thorough review of the potentially impacted folders and our internal files and systems in order to identify the information that was potentially impacted and to whom it related. In connection with this review, on or about December 11, 2020, a third-party firm was engaged to programmatically and manually review the large volume of files at issue to identify impacted individuals and the types of data associated with those individuals. Concurrently, Leaders Life internally reviewed their databases and, on or about March 31, 2021, first determined that one or more of the potentially impacted folders included protected information related to individuals.
>
> In conjunction and collaboration with the third-party review team, Leaders Life continued to diligently review the information and reconcile

[6] *Id.*

> the information with its internal records in furtherance of identifying the individuals to whom the data relates and the appropriate contact information for those individuals. These efforts were completed on or around May 19, 2021, at which time Leaders Life determined the scope of impacted individuals and the types of protected data associated with those individuals as a result of the extensive internal review.
>
> We thereafter worked to provide notification to potentially impacted individuals as quickly as possible. Importantly, there is no indication that your specific information was accessed or misused. However, we are notifying potentially impacted individuals out of an abundance of caution.
>
> **What Information was Involved?**
>
> Our investigation determined that the information related to you that may have been potentially affected includes your name, date of birth, Tax ID number, and/or Social Security number.

22. After receiving the Notice Letter, it is reasonable for recipients, including Plaintiff and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, in Leaders Life's letter, Defendant encourages impacted individuals to, among other things, "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." *See* **Exhibit 1**.

23. Indeed, Plaintiff's and Class Members' PII is now in the hands of cybercriminals who will use their PII to commit fraud and identity theft in order to profit off of the Data Breach.

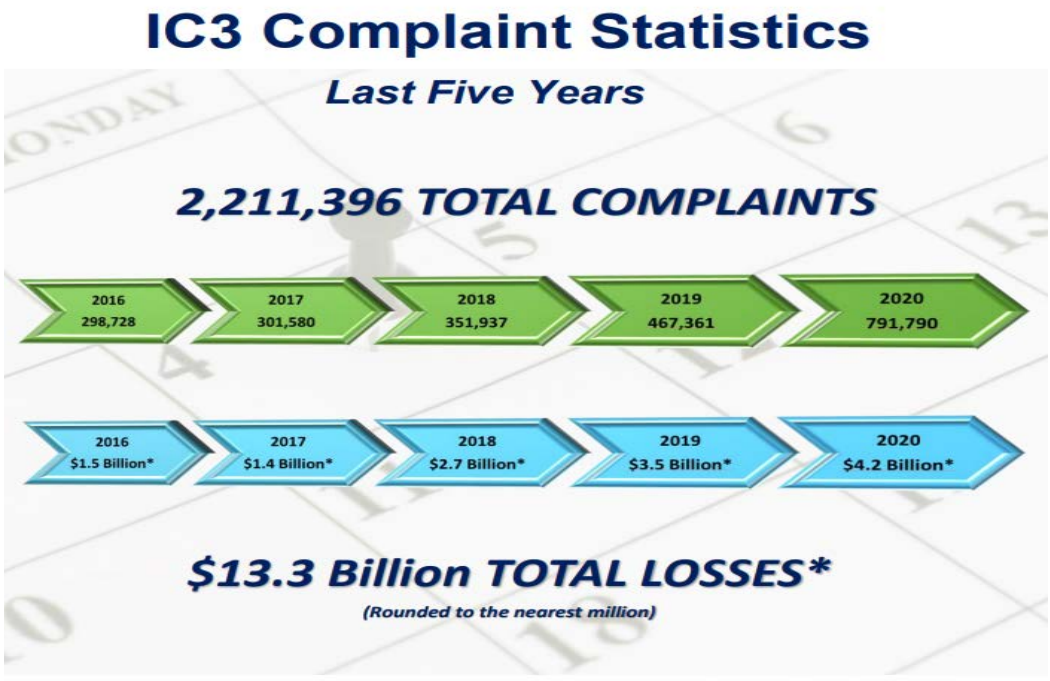
B. The PII exposed by Leaders Life as a result of its inadequate data security is highly valuable on the black market.

24. The information exposed by Leaders Life is a virtual goldmine for phishers,

hackers, identity thieves and cybercriminals.

25. Plaintiff and Class Members face real risks that must be brought to the Court's attention. These risks are the result of compromised PII being in the hands of cybercriminals and are the reason most circuit courts are now finding that data breach victims have Article III standing even if they have not yet fallen victim to identity theft.

26. This exposure of PII to cybercriminals is tremendously problematic and relevant here, where Plaintiff's and Class Members' PII is now in the hands of cybercriminals. As Leaders Life knows, cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2016 to 2020. Over that time, IC3 received a total of 2,211,396 complaints, reporting a loss of $13.3 billion.

27. By 2013, it was being reported that nearly one out of four data breach

notification recipients *becomes* a victim of identity fraud.[7]

28. Stolen PII like Plaintiff's and Class Members' PII is trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

29. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[8]

30. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about customers, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[9]

---

[7] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[8] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed June 1, 2021).

[9] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed June 1, 2021).

31. Even more troubling is the fact that PII is such a valuable commodity to identity thieves that, once it has been compromised, criminals will use it and trade the information on the cyber black market for years.[10]

32. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years after the data breach, by identity thieves to apply for COVID-19 related benefits here in the State of Oklahoma.[11]

33. The PII of consumers, including of Plaintiff and Class Members, remains of high value to criminals, as evidenced by the prices criminals will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

---

[10] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu

[11] *See https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[12] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 1, 2021).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 1, 2021).

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 1,

34. This was a financially motivated Data Breach, as apparent from the fact it was carried out by cybercriminals who will continue to seek to profit from the publishing and sale of Plaintiff's and Class Members' PII on the dark web.

35. Social Security numbers, which were part of the information compromised here, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[15]

36. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

37. Even then, a new Social Security number may not be effective. According to

---

2021).

[15] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 1, 2021).

Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

38. Because of this, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retail store data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

39. The PII compromised in the Data Breach commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[17]

40. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

41. According to the FBI's Internet Crime Complaint Center (IC3) 2020 Internet

[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 1, 2021).

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 1, 2021).

Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2020, resulting in more than $4.2 billion in losses to individuals and business victims.[18]

42. Further, rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good. Defendant failed to rapidly report to Plaintiff and Class Members that their PII had been stolen. It took Defendant months to even determine the information had been compromised, and then Plaintiff and Class Members were not notified until months after this determination was made that their PII had been accessed.

43. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

44. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

45. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[19] The GAO Report further notes that this type of identity fraud is the most

[18] *See* https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics (last accessed June 24, 2021).

[19] *See* Government Accountability Office, *Personal Information: Data Breaches are*

harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[20]

C. Leaders Life Failed to Comply with Federal Trade Commission Requirements.

46. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[21]

47. As Leaders Life knew or should have known, in 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[22] Among other things, the guidelines note businesses should properly dispose of personal

---

Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited June 1, 2021).

[20] *Id.*

[21] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 1, 2021).

[22] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 1, 2021).

information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

48. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[24]

49. Highlighting the importance of protecting against different types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[25]

50. Leaders Life was negligent in securing Plaintiff's and Class Members' PII

---

[23] *Id.*
[24] Federal Trade Commission, *Start With Security*, *supra footnote 17*.
[25] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 1, 2021).

by not implementing adequate data security and allowing an unknown third party to access Leaders Life's computer network in order to access unencrypted customer PII, Leaders Life failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data. Leaders Life's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

D. Plaintiff Legg's Experience

51. Plaintiff Legg has been a customer of Leaders Life for approximately twenty years.

52. On or around June 22, 2021, Plaintiff Legg received the Notice Letter from Leaders Life informing him of the Data Breach.

53. Plaintiff Legg has noticed a dramatic increase in the amount and frequency of phishing emails he has been receiving over the past few months.

54. As a result of the Data Breach, Plaintiff Legg has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through his unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options in addition to the free service offered by Defendant, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

55. Plaintiff Legg is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

56. Plaintiff Legg stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the few

online accounts that he has.

57. Additionally, Plaintiff Legg deletes electronic documents containing his PII and destroys documents that may contain any of his PII, or that may contain information that could otherwise be used to compromise his PII.

58. Plaintiff Legg has suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Legg entrusted to Defendant in order to purchase Defendant's insurance products and services. This PII was compromised in, and has been diminished as a result of, the Data Breach.

59. Plaintiff Legg also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces now that his PII is in the hands of cybercriminals.

60. Plaintiff Legg suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number and Tax ID number, in combination with his full name, which PII is now in the hands of cyber criminals and other unauthorized third parties who exfiltrated the PII with the intent of misusing it.

61. Knowing that thieves stole his PII, including his Social Security Number and Tax ID number and other PII that he was required to provide to Leaders Life, and knowing that his PII will be published and sold on the dark web, has caused Plaintiff Legg great stress and anxiety.

62. Plaintiff Legg has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

63. As a result of the Data Breach, Plaintiff Legg will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

64. Failing to adequately encrypt Plaintiff and Class Members PII was a basic function that Leaders Life failed to execute.

E. Plaintiff and the Class Members suffered damages.

65. The ramifications of Defendant's failure to keep current and former customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[26]

66. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

67. Defendant required Plaintiff and Class Members to provide their PII, including full names and Social Security numbers. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its

[26] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed June 1, 2021).

possession was only used to provide the agreed-upon insurance products and services from Defendant.

68. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendant, because their providing their PII was in exchange for Leaders Life's implied agreement to secure it and keep it safe.

69. The Data Breach was a direct and proximate result of Leaders Life's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

70. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former customers' PII.

71. Had Defendant remedied the deficiencies in its data security protocols and adopted adequate data security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

72. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and

family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

73. Plaintiff and Class Members have also had to deal with increased emotional distress and anxiety resulting from the substantial and imminent threat of fraud and identity theft they now face as a result of the Data Breach.

74. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[27]

75. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and/or are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

[27] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed June 1, 2021).

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

76. In addition to a remedy for the economic harm, Plaintiff and the Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

77. To date, other than providing a woefully inadequate twenty-four (24) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiff and Class Members other than simply telling them to review their financial records and credit reports on a regular basis.

78. This type of recommendation, however, does not require Defendant to expend any effort to protect Plaintiff's and Class Members' PII.

79. Defendant's failure to adequately protect Plaintiff's and Class Members' PII has resulted in Plaintiff and Class Members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's Notice Letter indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

80. Defendant's offer of twenty-four (24) months of identity monitoring and

identity protection services to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[28] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection. Although their PII was improperly exposed in or about the end of November 2020, affected current and former customers were not notified of the Data Breach until almost seven months later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Leaders Life's delay in detecting and notifying current and former customers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

74. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and the following proposed Nationwide Class, defined as follows:

> All persons residing in the United States who are current or former customers of Leaders Life or any Leaders Life affiliate, parent, or subsidiary, and received a Notice Letter stating that their PII may have

[28] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited June 1, 2021).

> been compromised as a result of the Data Breach that occurred between November 25, 2020 and November 27, 2020.

In addition, Plaintiff brings this action on behalf of himself and the following proposed Maryland Subclass defined as follows:

> All persons residing in the State of Maryland who are current or former customers of Leaders Life or any Leaders Life affiliate, parent, or subsidiary, and received a Notice Letter stating that their PII may have been compromised as a result of the Data Breach that occurred between November 25, 2020 and November 27, 2020.

75. Both the proposed Nationwide Class and the proposed Maryland Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

76. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Leaders Life; anyone employed by counsel in this action; and any judge to whom this case is assigned, including his or her spouse, and members of the judge's staff.

77. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

78. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the

Data Breach;

c. Whether Defendant owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PII in violation Section 5 of the FTC Act;

g. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

79. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

80. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the

Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

81. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

82. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence

(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Maryland Subclass)

83. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

84. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected.

85. Defendant owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former customers.

86. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former customers and exchanging it through email correspondence, and the critical importance of adequately securing such information.

87. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard it, that Defendant would not store it longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

88. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Defendant's misconduct included failing to implement the necessary systems, policies, customer training and procedures necessary to prevent the Data breach.

89. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

90. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

91. Plaintiff's injuries and damages, as described below, are a reasonably certain consequence of Leaders Life's breach of its duties.

92. Because Defendant knew that a breach of its systems would damage thousands of current and former Leaders Life customers whose PII was inexplicably contained, unencrypted, on its computer systems and networks, Defendant had a duty to adequately protect its data systems and the PII contained therein.

93. Defendant had a special relationship with current and former customers, including with Plaintiff and Class Members, by virtue of their being current or former customers. Plaintiff and Class Members reasonably believed that Defendant would take adequate security precautions to protect their PII. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and

Class Members' PII.

94. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class Members during the time it was within Defendant's possession or control.

95. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access and exfiltrate Leaders Life's customers' PII, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

96. Defendant's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

97. Neither Plaintiff nor Class Members contributed to the Data Breach as described in this Complaint.

98. As a direct and proximate cause of Defendant's actions and inactions, including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiff and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the theft and publication of their PII; (iii) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff, the Nationwide Class or, alternatively, the Maryland Subclass)

99. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

100. Defendant offered insurance products and services to its current and former customers, including Plaintiff and Class Members, in exchange for payment by Plaintiff and the Class for those insurance products.

101. As part of its business model, Defendant required Plaintiff and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, Tax ID numbers and other personal information, in order to obtain the insurance products and services at issue. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession would be protected from unauthorized access and viewing and would only be used to provide the agreed-upon insurance products and services.

102. These exchanges constituted an agreement between the parties: Plaintiff and Class Members would provide their PII in exchange for the insurance products and services provided by Defendant, including adequate data security and protection of Plaintiff's and Class Members' PII.

103. It is clear by these exchanges that the parties intended to enter into an agreement that included terms obligating Defendant to adequately safeguard Plaintiff's and Class Members' PII. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure and/or use.

104. Plaintiff and Class Members accepted Defendant's offer of insurance products and services and adequate data security, and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

105. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII.

106. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' PII.

107. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class Members violated the purpose of the agreement between the parties: Plaintiff's and Class Members' payment and PII in exchange for insurance products and services.

108. Defendant was on notice that its systems and data security protocols were inadequate yet failed to invest in the proper safeguarding of Plaintiff's and Class Members' PII.

109. Instead of spending the necessary financial resources to safeguard Plaintiff's and Class Members' PII, which Plaintiff and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class Members.

110. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

THIRD CAUSE OF ACTION
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Maryland Subclass)

111. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

112. As described above, when Plaintiff and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiff's and Class Members' PII and to timely detect and notify them in the event of a data breach.

113. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide payment and their PII in exchange for insurance products and services provided by Defendant.

114. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of insurance products and services. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members such insurance products and services.

115. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon insurance products and services from Defendant.

116. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendant, because their providing their PII was in exchange for Leaders Life's implied agreement to keep it safe and secure.

117. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

118. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII; storing the PII of current and former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with former customers; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendant's data security systems failed to meet applicable legal and industry standards.

119. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

120. Likewise, all conditions required for Defendant's performance were met.

121. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

122. Plaintiff and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual

identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

123. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific contractual term.

124. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

FOURTH CAUSE OF ACTION
Violation of the Maryland Consumer Protection Act
MD CODE ANN., COM. LAW § 13-301, et seq. ("MDTPA")
(On Behalf of Plaintiff Legg and the Maryland Subclass)

125. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

126. Section 13-301 of the Maryland Consumer Protection Act defines an unfair or deceptive trade practice, in relevant part, as the following:

> "Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with (i) The promotion or sale of any consumer goods, consumer realty, or consumer service…" Md. Code Ann., Com. Law § 13-301(9)(i).

127. Section 13-302 establishes that any prohibited practice under § 13-303 "is a violation of this title, whether or not any consumer in fact has been misled, deceived, or damaged as a result of that practice."

128. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the PII of Plaintiff and Maryland Subclass

Members, Leaders Life engaged in practices generally prohibited under Md. Code Ann., Com. Law § 13-303.

129. Leaders Life's conduct as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, its known concealment, suppression and omission of material facts relating to its inadequate data security practices and the occurrence of the Data Breach, with the intent that Plaintiff and members of the Maryland Subclass relied on the same omissions in connection with Leaders Life's promotion and sale of its insurance products.

130. Leaders Life's unfair and deceptive practices, including its known concealment, suppression and omission of material facts relating to the Data Breach, and its initial and ongoing omissions concerning its data security, materially induced Plaintiff and other members of the Maryland Subclass to pay more than they otherwise would have paid (if at all) had they known of Leaders Life's inadequate data security practices and that their PII was at risk of being compromised.

131. These deceptive practices caused Plaintiff and Maryland Subclass Members to suffer losses as set forth herein.

132. Leaders Life had a duty to disclose to Plaintiff and members of the Maryland Subclass that it did not and could not adequately protect sensitive PII. Leaders Life, as the party with knowledge of its data security shortcomings, knew that Plaintiff and members of the Maryland Subclass were entering transactions under a mistake as to the fact of its data security practice, and should have protected them accordingly.

133. Due to the Data Breach, Plaintiff and Maryland Subclass Members have lost

property in the form of the value of their PII and have suffered other actual damages. Further, Leaders Life's failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of its customers has resulted in Plaintiff and Maryland Subclass Members spending time monitoring their accounts. Plaintiff and Maryland Subclass Members are now at a higher and more substantial risk of identity theft crimes.

134. As a result of Leaders Life's practices, acts and omission, in violation of the MDTPA, Plaintiff and Maryland Subclass members have suffered injury-in-fact and have lost money or property. As a result of Leaders Life's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff and Maryland Subclass members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

135. Leaders Life's conduct proximately caused the injuries to Plaintiff and the Maryland Subclass and they are entitled to all damages, in addition to costs, interest and fees, including attorneys' fees, as allowed by law.

FIFTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiff and Nationwide Classes and Maryland Subclass)

136. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

137. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

138. As previously alleged, Plaintiff and Class Members entered into an implied

contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

139. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure their PII.

140. Defendant still possesses Plaintiff's and Class Members' PII and a risk of a second breach to Defendant's system is imminent and substantial.

141. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices that permitted the Data Breach to occur and, thereby, prevent future attacks.

142. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack. As such, Plaintiff and Class Members are at a substantial and imminent risk of having their PII compromised by cybercriminals once again through Defendant's inadequately secured data systems if their request for declaratory and injunctive relief is not granted.

143. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's ongoing failure to address the

security failings that led to such exposure.

144. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

145. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of himself and all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiff as Class Representative and the undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Leaders Life from engaging in the wrongful and unlawful acts described herein;

ii. requiring Leaders Life to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Leaders Life to delete, destroy, and purge the PII of Plaintiff and Class Members unless Leaders Life can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Leaders Life to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members' PII;

v. prohibiting Leaders Life from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

vi. requiring Leaders Life to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Leaders Life's systems on a periodic basis, and ordering Leaders Life to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Leaders Life to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Leaders Life to audit, test, and train its security personnel

regarding any new or modified procedures;

ix. requiring Leaders Life to segment data by, among other things, creating firewalls and access controls so that if one area of Leaders Life's network is compromised, hackers cannot gain access to other portions of Leaders Life's systems;

x. requiring Leaders Life to conduct regular database scanning and securing checks;

xi. requiring Leaders Life to establish an information security training program that includes at least annual information security training for all customers, with additional training to be provided as appropriate based upon the customers' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members,

xii. requiring Leaders Life to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Leaders Life to implement a system of tests to assess its respective customers' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing customers' compliance with Leaders Life's policies, programs, and systems for protecting PII;

xiv. requiring Leaders Life to implement, maintain, regularly review, and

revise as necessary a threat management program designed to appropriately monitor Leaders Life's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Leaders Life to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Leaders Life to implement logging and monitoring programs sufficient to track traffic to and from Leaders Life's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Leaders Life's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to detect and disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xxi. requiring Defendant's customers to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiff and Class Members damages;

f. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Date: September 28, 2021

Respectfully Submitted,

s/ William B. Federman

William B. Federman, OBA #2853
Tyler J. Bean, OBA #33834
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
meb@federmanlaw.com
tjb@federmanlaw.com

Attorneys for Plaintiff and the Class

CERTIFICATE OF SERVICE

I hereby certify that this document was filed through the ECF system and will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF), and paper copies will be sent to those indicated as non-registered participants on Tuesday, September 28, 2021.

/s/William B. Federman
William B. Federman